

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

SUBJECT DEVICES: Asus XZ205T Laptop, Dell Inspiron
15 Laptop, RCA Tablet, Dell T01C Tablet, Coolpad Cell
Phone, LG LGL64UL Cell Phone, LG M322X Cell Phone,
and Two Optical Discs

Case No. **MJ19-582**

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SUBJECT DEVICES: Further described in Attachment A, attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Title 18, U.S.C. § 2252(a)(2)
 Title 18, U.S.C. § 2252(a)(4)(B)

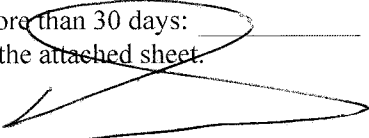
Offense Description

Receipt or Distribution of Child Pornography
 Possession of Child Pornography

The application is based on these facts:

See attached Affidavit

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

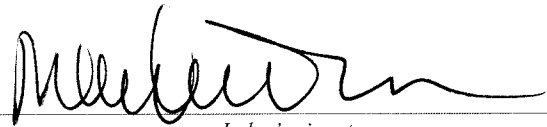

 Applicant's signature

Dan Huynh, Special Agent, HSI

Printed name and title

Sworn to before me pursuant to CrimRule 4.1.

Date: Dec. 4, 2019


 Judge's signature

City and state: Seattle, Washington

Hon. Mary Alice Theiler, U.S. Magistrate Judge

Printed name and title

2019R01168

AFFIDAVIT OF DAN HUYNH

STATE OF WASHINGTON)
) SS
COUNTY OF KING)

I, CAO TRIET (DAN) HUYNH, being first duly sworn on oath, depose and say:

I. INTRODUCTION

1. I am a Special Agent (SA) with the U.S. Department of Homeland Security, Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), assigned to the Special Agent in Charge (SAC), Seattle, Washington. I have been an agent with HSI since April 2010. HSI is responsible for enforcing the customs and immigration laws and federal criminal statutes of the United States. As part of my duties, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography and material involving the sexual exploitation of minors in violation of 18 U.S.C. §§ 2251, 2252, and 2252A.

2. I am a graduate of the Federal Law Enforcement Training Center (FLETC), ICE Special Agent Training Program, and have received further specialized training in investigating child pornography and child exploitation crimes. I have also had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256(8)). I have participated in the execution of previous search warrants, which involved child exploitation and/or child pornography offenses, and the search and seizure of computers, related peripherals, and computer media equipment. I am a member of the Seattle Internet Crimes Against Children Task Force, and work with other federal, state, and local law enforcement personnel in the investigation and prosecution of crimes involving the sexual exploitation of children. Before joining HSI, I worked for the City of Port Townsend, Washington, Police Department as a police officer and detective for approximately nine years.

1 3. I make this Affidavit in support of an application under Rule 41 of the
2 Federal Rules of Criminal Procedure for a warrant to search the following items more
3 fully described in Attachment A for the things specified in Attachment B:

- 4 a. Asus X205T Laptop
5 b. Dell Inspiron 15 Laptop
6 c. RCA Tablet
7 d. Dell T01C Tablet
8 e. Coolpad Cell Phone
9 f. LG LGL64UL Cell Phone
10 g. LG M322X Cell Phone
11 h. Two Optical Discs
12
13

14 The items to be searched (at times referred to as the "SUBJECT DEVICES"),
15 more fully described in Attachment A to this Affidavit, is currently located in the secure
16 office of the HSI Seattle, 1000 Second Avenue, Suite 2300, Seattle, Washington 98104.

17 4. The facts set forth in this Affidavit are based on my own personal
18 knowledge; knowledge obtained from other individuals during my participation in this
19 investigation, including other law enforcement officers; review of documents and records
20 related to this investigation; communications with others who have personal knowledge
21 of the events and circumstances described herein; and information gained through my
22 training and experience.

23 5. Because this Affidavit is submitted for the limited purpose of providing
24 sufficient facts necessary to determine whether there is probable cause in support of the
25 application for a search warrant, it does not set forth each and every fact that I or others
26 have learned during the course of this investigation. I have set forth only the facts that I
27 believe are relevant to the determination of probable cause to believe that evidence,
28 fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt/Distribution

1 of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography)
2 will be found on the SUBJECT DEVICES.

3 II. BACKGROUND

4 6. On or about February 27, 2009, CURTIS ALLEN RAPP was sentenced in
5 King County, Washington Superior Court by the Honorable Susan J. Craighead, Superior
6 Court Judge, to a minimum of 67 months imprisonment followed by lifetime supervised
7 release after being convicted of two counts of the Washington State crimes of Child
8 Molestation in the First Degree. According to the Certificate for Determination of
9 Probable Cause for this case, CURTIS ALLEN RAPP was working as a teacher at a
10 daycare, supervising children between the ages of 5-12 years old. CURTIS ALLEN
11 RAPP was charged and convicted of two counts of Child Molestation in the First Degree
12 when it was discovered that he had been touching and "tickling" a female child's genitals
13 both over and under her clothing for sexual gratification when the child was between 7
14 and 8 years old. It was alleged that there were at least two other victims of child
15 molestation in this case, but CURTIS ALLEN RAPP was only charged and convicted
16 based on accounts regarding one of the female children.

17 7. After CURTIS ALLEN RAPP was released from incarceration, he began
18 his lifetime Community Custody Supervision. CURTIS ALLEN RAPP was to abide by
19 conditions of supervision including, but not limited to, the following:
20

21 ///

22 ///

- 1 a. Obey all laws;
- 2 b. Do not initiate or prolong physical contact with children for any
- 3 reason;
- 4 c. Inform the Community Corrections Officer of any romantic
- 5 relationships to verify there are no victim-age children involved, and that the adult is
- 6 aware of your conviction history and conditions of supervision;
- 7 d. Have no contact with the victim or any minor-age children without
- 8 the approval of your Community Corrections Officer;
- 9 e. Do not possess or peruse pornographic materials unless given prior
- 10 approval by your sexual deviancy treatment specialist and/or Community Corrections
- 11 Officer. Pornographic materials are to be defined by the therapist and/or Community
- 12 Corrections Officer;
- 13 f. Do not attend X-rated movies, peep shows or adult bookstores
- 14 without the approval by your sexual deviancy treatment specialist or Community
- 15 Corrections Officer;
- 16 g. You must submit to a search of your person, residence, vehicle
- 17 and/or possessions when requested by a Community Corrections Officer. This includes
- 18 the search of your computer, cell phone and any other electronic devices.
- 19 8. On or about March 6, 2014, CURTIS ALLEN RAPP was released from
- 20 confinement, reported to the Washington State Department of Corrections (DOC) and
- 21 completed intake. At this time, CURTIS ALLEN RAPP signed the Conditions,
- 22 Requirements and Instructions form, the Acknowledgement of Drug/alcohol Testing -
- 23 Field form, the DOC Sex/Kidnap Registration Notification form, and additional intake
- 24 documents. A copy of all signed documents were provided to CURTIS ALLEN RAPP
- 25 for his records.
- 26 9. On or about July 7, 2014, CURTIS ALLEN RAPP completed an internet
- 27 safety plan with Community Sex Offender Treatment and Assessment Program provider,
- 28 Mark Hudson. This plan states the following:
"The reasons I need to use the internet are: job searches/applications, resumes,
Google maps, bus routes, online shopping, and email contact with family and
members of support group. I understand the dangers of poor internet usage. I will

1 not use peer to peer or social media and especially not porn. I will choose to
 2 navigate the internet wisely but to insure healthy choices - I will download
 3 blocking + monitor software. All unsolicited emails will remain unopened and
 4 then deleted. The internet is a most useful tool and also a privilege. I will use
 5 mindfulness and healthy coping skills to prevent abuse. I will discuss in group
 any breaches of conduct. Purchase a laptop - use only at public places, coffee
 house, etc."

6 10. On or about October 8, 2015, CURTIS ALLEN RAPP reported to the DOC
 7 to address concerns with polygraph testing that occurred on or about October 7, 2015,
 8 which indicated he was deceptive. CURTIS ALLEN RAPP acknowledged viewing
 9 sexually explicit materials on at least one occasion during the month of June 2015.
 10 CURTIS ALLEN RAPP was issued a Board Stipulated Agreement with the requirement
 11 that he successfully complete Moral Recognition Therapy (MRT) class, which he
 12 completed.

13 11. On or about July 28, 2017, CURTIS ALLEN RAPP submitted a Facebook
 14 Safety Plan to DOC Community Corrections Officer (CCO) Marco Lizarazo, which was
 15 approved the same day. This plan included the following information:

- 16 a. Build Community;
- 17 b. Keep socially active;
- 18 c. Keep in contact with family and friends;
- 19 d. Be a part of their lives in a positive way;
- 20 e. Share picture, thoughts, and ideas;
- 21 f. Build an online presence that can aid in getting jobs. As always, I
 22 know that the Internet is a great tool, but it can be a danger if used poorly. I will choose
 23 to use it wisely. Never have contact with minors or view porn. I will continue to use
 24 healthy coping skills and mindfulness so I may keep the privileges I have earned.
 25

26 12. On or about August 27, 2019, CCO Jenna Knox took over supervision of
 27 CURTIS ALLEN RAPP.

28 ///

III. SUMMARY OF INVESTIGATION

13. On or about September 24, 2019, CCO Knox and CCO Collin Young were conducting random home visits and made contact with CURTIS ALLEN RAPP at his apartment located in Seattle, Washington. CCO Knox introduced herself to CURTIS ALLEN RAPP and informed him that she would now be his supervising CCO. CURTIS ALLEN RAPP showed CCOs Knox and Young his one-bedroom apartment, and CCO Knox observed one smartphone and two laptops in plain view. CURTIS ALLEN RAPP was reminded of his next report date of September 27, 2019, and was given a copy of CCO Knox's business card with contact information in case he had any questions or concerns.

14. On or about September 27, 2019, CURTIS ALLEN RAPP reported to the DOC as directed. During the meeting, CURTIS ALLEN RAPP confirmed his address and the fact that he does not have any roommates. CCO Knox then proceeded to review CURTIS ALLEN RAPP's conditions of supervision. During their conversation, CURTIS ALLEN RAPP disclosed he installed Internet monitoring software on his electronic devices while in Community Sex Offender Treatment and Assessment, but had not used the monitoring software since completing treatment. CCO Knox asked CURTIS ALLEN RAPP what electronic devices he owned, and CURTIS ALLEN RAPP advised he owned one cell phone and one laptop. CCO Knox asked if he had any other electronic devices that are capable of Internet use and CURTIS ALLEN RAPP stated that he had "a few" old phones that he doesn't use anymore. A check of CURTIS ALLEN RAPP's field file revealed no documentation approving CURTIS ALLEN RAPP to have unmonitored Internet access. CURTIS ALLEN RAPP's Internet safety plan indicated he would need to download monitoring software on all electronic devices.

15. Due to CCO Knox having observed CURTIS ALLEN RAPP having two laptops and one smartphone in his room just three days prior, CCO Knox had reasonable suspicion to believe that CURTIS ALLEN RAPP was in violation of his conditions due to having Internet capable electronic devices that were not approved by a CCO and not

1 monitored by software. CCO Knox briefed the situation with Community Corrections
2 Supervisor (CCS) Michelle Kaiser, who approved of a search of CURTIS ALLEN
3 RAPP's electronic devices and a search of his residence.

4 16. CCO Knox searched the LG cell phone Model LGM322, IMEI
5 #357105082054129 CURTIS ALLEN RAPP had with him. It was discovered that
6 CURTIS ALLEN RAPP was searching phrases such as "Kristen Stewart Nude" and
7 "Abigail Breslin Nude."

8 17. CURTIS ALLEN RAPP was searched for officer safety and placed in the
9 DOC vehicle. CURTIS ALLEN RAPP was transported to his residence, and a search of
10 his one-bedroom apartment was completed by CCOs Knox and Sean Santiago. The
11 following items (the rest of the SUBJECT DEVICES) were discovered during the search,
12 removed from the residence and secured at the DOC Seattle Office:

- 13 a. Asus X205T Laptop with sticker #FANLCX21355443C;
- 14 b. Dell Inspiron 15 Laptop with service tag #G7BQ4L2;
- 15 c. RCA Tablet with serial number #AWFDFZ0006M3;
- 16 d. Dell T01C Tablet (unable to locate serial number);
- 17 e. Coolpad Cell Phone with IMEI #863519031152742;
- 18 f. LG LGL64UL Cell Phone with IMEI #353261081249550;
- 19 g. Charging chord for laptop Charging chord for phones; and
- 20 h. Two (2) DVD/CD discs.

21
22
23 18. CURTIS ALLEN RAPP was transported back to CCO Knox's office and
24 directed to sit in the lobby while a search of the SUBJECT DEVICES was conducted.

25 19. The Asus laptop was searched by CCO Knox, to include a search of the
26 Internet browser search history. CURTIS ALLEN RAPP's browser search history
27 indicated daily use of this device. CCO Knox also took photographs, while searching this
28

1 Asus laptop. There were numerous searches on the Bing.com photo and video search
2 engine, including but not limited to the following search terms:

- 3 a. Reluctant Teen Seduced by Lesbian Mas...;
- 4 b. Little Bitch Album Collection vids;
- 5 c. Toddlercon;
- 6 d. Jr naturists;
- 7 e. Zombie Girl gest Ass Fucked;
- 8 f. Female high school tennis; and
- 9 g. Prettiest Girls in Tennis Ball.

10
11
12 20. CCO Knox found other searches and websites that CURTIS ALLEN RAPP
13 visited that included the following:

- 14 a. 3D lolicon animation - Lolicon Hentai: 3;
- 15 b. Old women sex with boys - Picsninja.com;
- 16 c. Big cock boys nudist camp – Picsninja.com;
- 17 d. Sweetie_rinushka_at Chaturbate: Lovens...;
- 18 e. Chaturbate Full Video Mode;
- 19 f. Toddler Porn Videos Pornhub.com;
- 20 g. Schoolgirl Handjob and Foreskin 4K - P...;
- 21 h. 4K Sex with a Schoolgirl who Likes the S...;
- 22 i. Very Very Skinny Young Fuck Porn Video...; and
- 23 j. Lesbian Teacher Has Student Stay after...

24
25
26 21. CCO Knox clicked on a link CURTIS ALLEN RAPP viewed titled,
27 "Toddler Porn Videos Pornhub.com" and a screen showed up that read, "Most Relevant
28 Video Results: Toddler." This list of suggested videos included links to titles including

1 "cummy yummy toddler baby dick," "massive cum shot all over innocent toddler,"
2 "Dropbox links & megalinks," "Ebony Mommy Demotes Sissy Pull Up Toddler to Sissy
3 Diaper Baby In," and "camera toddler shows her trousers nude."

4 22. CCO Knox next clicked on a link CURTIS ALLEN RAPP viewed titled,
5 "3D lolicon animation - Lolicon Hentai: 3...". The website that opened showed an
6 animated graphic of a naked prepubescent female child at the top of the page, and a
7 description for the "Mimic72 3D Lolicon Collection Vol.7" scheduled for 9/3/2019. The
8 description states "New very hot and cool 3D location collection that includes 14 very hot
9 3D animations. Hot lolitas with camel toe vaginas then ride their daddy's big hard dicks
10 on the beach. Enjoy! Also, don't miss the other volumes! Type: lolicon 3D Images and
11 gifs. Author: Mimic 72. 31 pies 14 gifs."

12 23. Among a Bing.com image search for "toddlercon," several image results
13 were provided. Most of these search results depicted prepubescent children engaged
14 in graphic sexual behavior. Some of these images were clearly anime or digitally
15 produced. The following described image was unclear whether it was a real picture
16 or a high-quality animation:

17 The image depicts a prepubescent female child, approximately 3 to 5
18 years old, lying nude on a blue patterned material. The child is facing
19 the camera and has her hands covering her nipples. The child's legs are
20 bent at the knees and spread apart exposing her vagina to the camera.
21 Kneeling in front of the child is an adult male depicted nude from the
22 abdomen down. The adult's erect penis is positioned between the child's
23 legs, above her vagina.

24 24. Among a Bing.com image search for "jr naturists," several image results
25 were provided. Among these results, one of the links that was visited depicted a
26 prepubescent female probably approximately 9-11 years old depicted standing
27 completely nude in a bathroom. This image depicts her exposed chest and nipples as well
28

1 as her vagina and labia. While blocked by a shower door, there appears to be an adult
2 standing behind her in the shower.¹

3 25. I reviewed the photos that CCO Knox took of the search of CURTIS
4 ALLEN RAPP's Asus laptop and confirmed the Internet browsing history and images
5 that were found above. I concur with all the findings and descriptions that CCO Knox
6 made above.

7 26. After reviewing these aspects of Mr. Rapp's internet search history, it was
8 determined that CURTIS ALLEN RAPP was in violation of his conditions of Community
9 Custody Supervision and would be arrested for these violations. The search of CURTIS
10 ALLEN RAPP's SUBJECT DEVICES was paused. The SUBJECT DEVICES were
11 packaged as evidence and secured in the Seattle Metro Unit Temporary Evidence Locker
12 #3 (DOC Seattle). When CCOs went to arrest CURTIS ALLEN RAPP, it was
13 discovered that he had left the lobby. CCOs walked the perimeter of the building looking
14 for CURTIS ALLEN RAPP, and subsequently went to CURTIS ALLEN RAPP's
15 residence looking for him. CURTIS ALLEN RAPP was not located. A DOC warrant
16 was issued for CURTIS ALLEN RAPP's arrest, and as of this time, he has not been
17 located.

18 27. On or about October 18, 2019, I arrived at the DOC Office in Seattle,
19 Washington, and met with CCO Knox. I confirmed and obtained additional details of
20 CCO Knox's involvement of the case and took custody of the SUBJECT DEVICES. I
21 also obtained the photographs CCO Knox took of the searches of CURTIS ALLEN
22 RAPP's LG Android cell phone model M322X, IMEI #357105082054129 and Asus
23 laptop.

24 ///

25 ///

26 _____
27 ¹ Copies of the two described images will be provided to the reviewing magistrate judge as part of this application in
28 an envelope marked Exhibit 1. Should this application be granted, Exhibit 1 will not be filed with the Court but
instead remain in the custody of HSI in the event it is relevant to future legal proceedings related to this
investigation.

28. The SUBJECT DEVICES were not manufactured in the state of Washington. All the SUBJECT DEVICES excluding the two optical discs included labels/markings stating they were all made in China.

IV. DEFINITIONS AND TECHNICAL TERMS

29. Set forth below are some definitions of technical terms, most of which are used throughout this Affidavit pertaining to the Internet and computers generally:

a. Computers and digital devices: As used in this Affidavit, the terms “computer” and “digital device,” along with the terms “electronic storage media,” “digital storage media,” and “data storage device,” refer to those items capable of storing, creating, transmitting, displaying, or encoding electronic or digital data, including computers, hard drives, thumb drives, flash drives, memory cards, media cards, smart cards, PC cards, digital cameras and digital camera memory cards, electronic notebooks and tablets, smart phones and personal digital assistants, printers, scanners, and other similar items.

b. Internet Service Providers (ISPs) and the storage of ISP records: Internet Service Providers are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e mail, remote storage, and co-location of computers and other communications equipment. ISPs maintain records (“ISP records”) pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e mail communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use.

c. Internet Protocol (IP) Address: Typically, computers or devices on the Internet are referenced by a unique Internet Protocol address the same way every

1 telephone has a unique telephone number. An IP address consists of four numeric
2 sequences, separated by a period, and each numeric sequence is a whole number between
3 0 and 254. An example of an IP address is 192.168.10.102. Each time an individual
4 accesses the Internet, the computer from which that individual initiates access is assigned
5 an IP address. A central authority provides each ISP a limited block of IP addresses for
6 use by that ISP's customers or subscribers. Most ISP's employ dynamic IP addressing,
7 that is, they allocate any unused IP address at the time of initiation of an Internet session
8 each time a customer or subscriber accesses the Internet. A dynamic IP address is
9 reserved by an ISP to be shared among a group of computers over a period of time. The
10 ISP logs the date, time, and duration of the Internet session for each IP address and can
11 identify the user of that IP address for such a session from these records. Typically, users
12 who sporadically access the Internet via a dial up modem will be assigned an IP address
13 from a pool of IP addresses for the duration of each dial up session. Once the session
14 ends, the IP address is available for the next dial up customer. On the other hand, some
15 ISPs, including some cable providers, employ static IP addressing, that is, a customer or
16 subscriber's computer is assigned one IP address that is used to identify each and every
17 Internet session initiated through that computer. In other words, a static IP address is an
18 IP address that does not change over a period of time and is typically assigned to a
19 specific computer.

20 d. Hash Value: "Hashing" refers to the process of using a
21 mathematical function, often called an algorithm, to generate a numerical identifier for
22 data. This numerical identifier is called a "hash value" and can be thought of as a "digital
23 fingerprint" for data. If the data that has been "hashed" is changed, even very slightly
24 (like through the addition or deletion of a comma or a period in a text file), the hash value
25 for that data would change. Therefore, if a file such as a digital photo is a hash value
26 match to a known file, it means that the digital photo is an exact copy of the known file.

27 ///

28 ///

V. TECHNICAL BACKGROUND

30. As part of my training, I have become familiar with the Internet, a global network of computers and other electronic devices that communicate with each other using various means, including standard telephone lines, high speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions, including satellite. Due to the structure of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via email.

31. I know, based on my training and experience, that cellular phones (referred to generally as "smart phones") have the capability to access the Internet and store information, such as videos and images. As a result, an individual using a smart phone can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smart phone can also easily plug the device into a computer, via a USB cable, and transfer data files from one digital device to another. Many people generally carry their smart phone on their person; recent investigations in this District have resulted in the discovery of child pornography files on smart phones which were carried on an individual's person at the time the phones were seized.

32. As set forth above and in Attachment B to this Affidavit, I seek permission to search for and seize evidence, fruits, and instrumentalities of the above-referenced crimes that might be on the SUBJECT DEVICES, in whatever form they are found. It has been my experience that individuals involved in child pornography often prefer to store images of child pornography in electronic form. The ability to store images of child pornography in electronic form makes digital devices, examples of which are enumerated in Attachment B to this Affidavit, an ideal repository for child pornography because the

1 images can be easily sent or received over the Internet. As a result, one form in which
2 these items may be found is as electronic evidence stored on a digital device.

3 a. Based upon my knowledge, training, and experience in child
4 exploitation and child pornography investigations, and the experience and training of
5 other law enforcement officers with whom I have had discussions, I know that computers
6 and computer technology have revolutionized the way in which child pornography is
7 collected, distributed, and produced. Prior to the advent of computers and the Internet,
8 child pornography was produced using cameras and film, resulting in either still
9 photographs or movies. The photographs required darkroom facilities and a significant
10 amount of skill in order to develop and reproduce the images. As a result, there were
11 definable costs involved with the production of pornographic images. To distribute these
12 images on any scale also required significant resources. The photographs themselves
13 were somewhat bulky and required secure storage to prevent their exposure to the public.
14 The distribution of these images was accomplished through a combination of personal
15 contacts, mailings, and telephone calls, and compensation would follow the same paths.
16 More recently, through the use of computers and the Internet, distributors of child
17 pornography use membership based/subscription based websites to conduct business,
18 allowing them to remain relatively anonymous.

19 b. In addition, based upon my own knowledge, training, and experience
20 in child exploitation and child pornography investigations, and the experience and
21 training of other law enforcement officers with whom I have had discussions, I know that
22 the development of computers has also revolutionized the way in which those who seek
23 out child pornography are able to obtain this material. Computers serve four basic
24 functions in connection with child pornography: production, communication, distribution,
25 and storage. More specifically, the development of computers has changed the methods
26 used by those who seek to obtain access to child pornography as described in
27 subparagraphs (c) through (f) below.

1 c. Producers of child pornography can now produce both still and
2 moving images directly from the average video or digital camera. These still and/or
3 moving images are then uploaded from the camera to the computer, either by attaching
4 the camera to the computer through a USB cable or similar device, or by ejecting the
5 camera memory card from the camera and inserting it into a card reader. Once uploaded
6 to the computer, the images can then be stored, manipulated, transferred, or printed
7 directly from the computer. Images can be edited in ways similar to those by which a
8 photograph may be altered. Images can be lightened, darkened, cropped, or otherwise
9 manipulated. Producers of child pornography can also use a scanner to transfer printed
10 photographs into a computer-readable format. As a result of this technology, it is
11 relatively inexpensive and technically easy to produce, store, and distribute child
12 pornography. In addition, there is an added benefit to the pornographer in that this
13 method of production does not leave as large a trail for law enforcement to follow.

14 d. The Internet allows any computer to connect to another computer.
15 By connecting to a host computer, electronic contact can be made to literally millions of
16 computers around the world. A host computer is one that is attached to a network and
17 serves many users. Host computers, including ISPs, allow email service between
18 subscribers and sometimes between their own subscribers and those of other networks.
19 In addition, these service providers act as a gateway for their subscribers to the Internet.
20 Having said that, however, this application does not seek to reach any host computers.
21 This application seeks permission only to search the SUBJECT DEVICES.

22 e. The Internet allows users, while still maintaining anonymity, to
23 easily locate (i) other individuals with similar interests in child pornography, and (ii)
24 websites that offer images of child pornography. Those who seek to obtain images or
25 videos of child pornography can use standard Internet connections, such as those
26 provided by businesses, universities, and government agencies, to communicate with
27 each other and to distribute child pornography. These communication links allow
28 contacts around the world as easily as calling next door. Additionally, these

1 communications can be quick, relatively secure, and as anonymous as desired. All of
2 these advantages, which promote anonymity for both the distributor and recipient, are
3 well known and are the foundation of transactions involving those who wish to gain
4 access to child pornography over the Internet. Sometimes the only way to identify both
5 parties and verify the transportation of child pornography over the Internet is to examine
6 the distributor's/recipient's computer, including the Internet history and cache to look for
7 "footprints" of the websites and images accessed by the distributor/recipient.

8 f. The computer's capability to store images in digital form makes it an
9 ideal repository for child pornography. The size of the electronic storage media
10 (commonly referred to as a "hard drive") used in home computers has grown
11 tremendously within the last several years. Hard drives with the capacity of 2 terabytes
12 are not uncommon. These drives can store thousands of images at very high resolution.
13 Magnetic storage located in host computers adds another dimension to the equation. It is
14 possible to use a video camera to capture an image, process that image in a computer
15 with a video capture board, and save that image to storage elsewhere. Once this is done,
16 there is no readily apparent evidence at the "scene of the crime." Only with careful
17 laboratory examination of electronic storage devices is it possible to recreate the evidence
18 trail.

19 33. Based upon my knowledge, experience, and training in child pornography
20 investigations, and the training and experience of other law enforcement officers with
21 whom I have had discussions, I know that there are certain characteristics common to
22 individuals who have a sexualized interest in children and depictions of children:

23 a. They may receive sexual gratification, stimulation, and satisfaction
24 from contact with children; or from fantasies they may have viewing children engaged in
25 sexual activity or in sexually suggestive poses, such as in person, in photographs, or other
26 visual media; or from literature describing such activity.

27 b. They may collect sexually explicit or suggestive materials in a
28 variety of media, including photographs, magazines, motion pictures, videotapes, books,

1 slides, and/or drawings or other visual media. Such individuals often times use these
2 materials for their own sexual arousal and gratification. Further, they may use these
3 materials to lower the inhibitions of children they are attempting to seduce, to arouse the
4 selected child partner, or to demonstrate the desired sexual acts. These individuals may
5 keep records, to include names, contact information, and/or dates of these interactions, of
6 the children they have attempted to seduce, arouse, or with whom they have engaged in
7 the desired sexual acts.

8 c. They often maintain any "hard copies" of child pornographic
9 material that is, their pictures, films, video tapes, magazines, negatives, photographs,
10 correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of
11 their home or some other secure location. These individuals typically retain these "hard
12 copies" of child pornographic material for many years, as they are highly valued.

13 d. Likewise, they often maintain their child pornography collections
14 that are in a digital or electronic format in a safe, secure and private environment, such as
15 a computer and surrounding area. These collections are often maintained for several
16 years and are kept close by, often at the individual's residence or some otherwise easily
17 accessible location, to enable the owner to view the collection, which is valued highly.
18 They also may opt to store the contraband in cloud accounts. Cloud storage is a model of
19 data storage where the digital data is stored in logical pools, the physical storage can span
20 multiple servers, and often locations, and the physical environment is typically owned
21 and managed by a hosting company. Cloud storage allows the offender ready access to
22 the material from any device that has an Internet connection, worldwide, while also
23 attempting to obfuscate or limit the criminality of possession as the material is stored
24 remotely and not on the offender's device.

25 e. They also may correspond with and/or meet others to share
26 information and materials; rarely destroy correspondence from other child pornography
27 distributors/collectors; conceal such correspondence as they do their sexually explicit
28 material; and often maintain lists of names, addresses, and telephone numbers of

1 individuals with whom they have been in contact and who share the same interests in
2 child pornography.

3 f. They generally prefer not to be without their child pornography for
4 any prolonged time period. This behavior has been documented by law enforcement
5 officers involved in the investigation of child pornography throughout the world.

6 34. In addition to offenders who collect and store child pornography, law
7 enforcement has encountered offenders who obtain child pornography from the internet,
8 view the contents and subsequently delete the contraband, often after engaging in self-
9 gratification. In light of technological advancements, increasing Internet speeds and
10 worldwide availability of child sexual exploitative material, this phenomenon offers the
11 offender a sense of decreasing risk of being identified and/or apprehended with quantities
12 of contraband. This type of consumer is commonly referred to as a 'seek and delete'
13 offender, knowing that the same or different contraband satisfying their interests remain
14 easily discoverable and accessible online for future viewing and self-gratification. I
15 know that, regardless of whether a person discards or collects child pornography he/she
16 accesses for purposes of viewing and sexual gratification, evidence of such activity is
17 likely to be found on computers and related digital devices, including storage media, used
18 by the person. This evidence may include the files themselves, logs of account access
19 events, contact lists of others engaged in trafficking of child pornography, backup files,
20 and other electronic artifacts that may be forensically recoverable.

21 35. Given the above-stated facts, including CURTIS ALLEN RAPP's criminal
22 histories and the findings of the DOC and based on my knowledge, training and
23 experience, along with my discussions with other law enforcement officers who
24 investigate child exploitation crimes, I believe that CURTIS ALLEN RAPP likely has a
25 sexualized interest in children and depictions of children and that evidence of child
26 pornography is likely to be found on the SUBJECT DEVICES.

27 36. Based on my training and experience, and that of computer forensic agents
28 that I work and collaborate with on a daily basis, I know that every type and kind of

1 information, data, record, sound or image can exist and be present as electronically stored
2 information on any of a variety of computers, computer systems, digital devices, and
3 other electronic storage media. I also know that electronic evidence can be moved easily
4 from one digital device to another. As a result, I believe that electronic evidence may be
5 stored on the SUBJECT DEVICES.

6 37. Based on my training and experience, and my consultation with computer
7 forensic agents who are familiar with searches of computers, I know that in some cases
8 the items set forth in Attachment B may take the form of files, documents, and other data
9 that is user-generated and found on a digital device. In other cases, these items may take
10 the form of other types of data – including in some cases data generated automatically by
11 the devices themselves.

12 38. Based on my training and experience, and my consultation with computer
13 forensic agents who are familiar with searches of computers, I believe that regarding any
14 digital devices recovered from CURTIS ALLEN RAPP there is probable cause to believe
15 that the items set forth in Attachment B will be stored in the SUBJECT DEVICES for a
16 number of reasons, including but not limited to the following:

17 a. Once created, electronically stored information (ESI) can be stored
18 for years in very little space and at little or no cost. A great deal of ESI is created, and
19 stored, moreover, even without a conscious act on the part of the device operator. For
20 example, files that have been viewed via the Internet are sometimes automatically
21 downloaded into a temporary Internet directory or “cache,” without the knowledge of the
22 device user. The browser often maintains a fixed amount of hard drive space devoted to
23 these files, and the files are only overwritten as they are replaced with more recently
24 viewed Internet pages or if a user takes affirmative steps to delete them. This ESI may
25 include relevant and significant evidence regarding criminal activities, but also, and just
26 as importantly, may include evidence of the identity of the device user, and when and
27 how the device was used. Most often, some affirmative action is necessary to delete ESI.

1 And even when such action has been deliberately taken, ESI can often be recovered,
2 months or even years later, using forensic tools.

3 b. Wholly apart from data created directly (or indirectly) by user-
4 generated files, digital devices – in particular, a computer’s internal hard drive – contain
5 electronic evidence of how a digital device has been used, what it has been used for, and
6 who has used it. This evidence can take the form of operating system configurations,
7 artifacts from operating systems or application operations, file system data structures, and
8 virtual memory “swap” or paging files. Computer users typically do not erase or delete
9 this evidence, because special software is typically required for that task. However, it is
10 technically possible for a user to use such specialized software to delete this type of
11 information – and, the use of such special software may itself result in ESI that is relevant
12 to the criminal investigation. HSI agents in this case have consulted on computer
13 forensic matters with law enforcement officers with specialized knowledge and training
14 in computers, networks, and Internet communications. In particular, to properly retrieve
15 and analyze electronically stored (computer) data, and to ensure accuracy and
16 completeness of such data and to prevent loss of the data either from accidental or
17 programmed destruction, it is necessary to conduct a forensic examination of the
18 computers. To effect such accuracy and completeness, it may also be necessary to
19 analyze not only data storage devices, but also peripheral devices which may be
20 interdependent, the software to operate them, and related instruction manuals containing
21 directions concerning operation of the computer and software.

22 **VI. SEARCH AND/OR SEIZURE OF DIGITAL DEVICES**

23 39. In addition, based on my training and experience and that of computer
24 forensic agents that I work and collaborate with on a daily basis, I know that in most
25 cases it is impossible to successfully conduct a complete, accurate, and reliable search for
26 electronic evidence stored on a digital device during the physical search of a search site
27 for a number of reasons, including but not limited to the following:
28

1 a. Technical Requirements: Searching digital devices for criminal
2 evidence is a highly technical process requiring specific expertise and a properly
3 controlled environment. The vast array of digital hardware and software available
4 requires even digital experts to specialize in particular systems and applications, so it is
5 difficult to know before a search which expert is qualified to analyze the particular
6 system(s) and electronic evidence found at a search site. As a result, it is not always
7 possible to bring to the search site all of the necessary personnel, technical manuals, and
8 specialized equipment to conduct a thorough search of every possible digital
9 device/system present. In addition, electronic evidence search protocols are exacting
10 scientific procedures designed to protect the integrity of the evidence and to recover even
11 hidden, erased, compressed, password-protected, or encrypted files. Since ESI is
12 extremely vulnerable to inadvertent or intentional modification or destruction (both from
13 external sources or from destructive code embedded in the system such as a “booby
14 trap”), a controlled environment is often essential to ensure its complete and accurate
15 analysis.

16 b. Volume of Evidence: The volume of data stored on many digital
17 devices is typically so large that it is impossible to search for criminal evidence in a
18 reasonable period of time during the execution of the physical search of a search site. A
19 single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A
20 single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000
21 double-spaced pages of text. Computer hard drives are now being sold for personal
22 computers capable of storing up to two terabytes (2,000 gigabytes of data.) Additionally,
23 this data may be stored in a variety of formats or may be encrypted (several new
24 commercially available operating systems provide for automatic encryption of data upon
25 shutdown of the computer).

26 c. Search Techniques: Searching the ESI for the items described in
27 Attachment B may require a range of data analysis techniques. In some cases, it is
28 possible for agents and analysts to conduct carefully targeted searches that can locate

1 evidence without requiring a time-consuming manual search through unrelated materials
2 that may be commingled with criminal evidence. In other cases, however, such
3 techniques may not yield the evidence described in the warrant, and law enforcement
4 personnel with appropriate expertise may need to conduct more extensive searches, such
5 as scanning areas of the disk not allocated to listed files, or peruse every file briefly to
6 determine whether it falls within the scope of the warrant.

7 40. In this particular case, the government anticipates the use of a hash value
8 library to exclude normal operating system files that do not need to be searched, which
9 will facilitate the search for evidence that does come within the items described in
10 Attachment B. Further, the government anticipates the use of hash values and known file
11 filters to assist the digital forensics examiners/agents in identifying known and or
12 suspected child pornography image files. Use of these tools will allow for the quick
13 identification of evidentiary files but also assist in the filtering of normal system files that
14 would have no bearing on the case.

15 41. In accordance with the information in this Affidavit, law enforcement
16 personnel will execute the search of digital devices seized pursuant to this warrant as
17 follows:

18 a. In order to examine the ESI in a forensically sound manner, law
19 enforcement personnel with appropriate expertise will produce a complete forensic
20 image, if possible and appropriate, of any digital device that is found to contain data or
21 items that fall within the scope of Attachment B of this Affidavit. In addition,
22 appropriately trained personnel may search for and attempt to recover deleted, hidden, or
23 encrypted data to determine whether the data fall within the list of items to be seized
24 pursuant to the warrant. In order to search fully for the items identified in the warrant,
25 law enforcement personnel, which may include investigative agents, may then examine
26 all of the data contained in the forensic image/s and/or on the digital devices to view their
27 precise contents and determine whether the data fall within the list of items to be seized
28 pursuant to the warrant.

1 b. The search techniques that will be used will be only those methodologies,
2 techniques and protocols as may reasonably be expected to find, identify, segregate
3 and/or duplicate the items authorized to be seized pursuant to Attachment B to this
4 Affidavit.

5 c. If, after conducting its examination, law enforcement personnel determine
6 that any digital device is an instrumentality of the criminal offenses referenced above, the
7 government may retain that device during the pendency of the case as necessary to,
8 among other things, preserve the instrumentality evidence for trial, ensure the chain of
9 custody, and litigate the issue of forfeiture.

10 42. In order to search for ESI that falls within the list of items to be seized
11 pursuant to Attachment B to this Affidavit, law enforcement personnel will seize and
12 search the following items (heretofore and hereinafter referred to as "digital devices"),
13 subject to the procedures set forth above:

14 a. Any digital device capable of being used to commit, further, or store
15 evidence of the offense(s) listed above;

16 b. Any digital device used to facilitate the transmission, creation,
17 display, encoding, or storage of data, including word processing equipment, modems,
18 docking stations, monitors, printers, cameras, encryption devices, and optical scanners;

19 c. Any magnetic, electronic, or optical storage device capable of
20 storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or
21 memory buffers, smart cards, PC cards, memory sticks, flashdrives, thumb drives, camera
22 memory cards, media cards, electronic notebooks, and personal digital assistants;

23 d. Any documentation, operating logs and reference manuals regarding
24 the operation of the digital device, or software;

25 e. Any applications, utility programs, compilers, interpreters, and other
26 software used to facilitate direct or indirect communication with the device hardware, or
27 ESI to be searched;
28

1 f. Any physical keys, encryption devices, dongles and similar physical
2 items that are necessary to gain access to the digital device, or ESI; and

3 g. Any passwords, password files, test keys, encryption codes or other
4 information necessary to access the digital device or ESI.

5 **VII. INSTRUMENTALITIES**

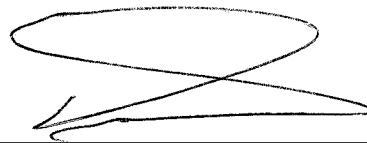
6 43. Based on the information in this Affidavit, I also believe that the SUBJECT
7 DEVICES are instrumentalities of crime and constitute the means by which violations of
8 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. §
9 2252(a)(4)(B) (Possession of Child Pornography) have been committed. Therefore, I
10 believe that in addition to seizing the digital devices to conduct a search of their contents
11 as set forth herein, there is probable cause to seize those digital devices as
12 instrumentalities of criminal activity.

13
14 ///

15 ///

VIII. CONCLUSION

44. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) are located on the SUBJECT DEVICES, as more fully described in Attachment A to this Affidavit, as well as on and in any digital devices found therein. I therefore request that the court issue a warrant authorizing a search of the SUBJECT DEVICES, for the items more fully described in Attachment B hereto, incorporated herein by reference, and the seizure of any such items found therein.



CAO TRIET (DAN) HUYNH,
Affiant, Special Agent
Department of Homeland Security
Homeland Security Investigations

SUBSCRIBED and SWORN to before me this 4 day of December, 2019. In addition to the foregoing affidavit, I have also reviewed the contents of Exhibit 1. Upon completing that review, the contents of Exhibit 1 were returned to the envelope labeled Exhibit 1. The envelope was sealed, and I placed my signature across the seal.



HON. MARY ALICE THEILER
United States Magistrate Judge

ATTACHMENT A

ITEMS TO BE SEARCHED

The following item to be searched and subsequently forensically examined is currently in the custody of HSI Seattle and was detained by Washington State Department of Corrections on or about October 18, 2019, from CURTIS RAPP and is currently located in the secure office of HSI Seattle at 1000 Second Avenue, Suite 2300, Seattle, Washington 98104:

Asus X205T Laptop with sticker #FANLCX21355443C

Dell Inspiron 15 Laptop with service tag #G7BQ4L2

RCA Tablet with serial number #AWFDFZ0006M3

Dell T01C Tablet

Coolpad Cell Phone with IMEI #863519031152742

LG LGL64UL Cell Phone with IMEI #353261081249550

LG M322X Cell Phone with IMEI #357105082054129

Two Optical Discs

ATTACHMENT B**ITEMS TO BE SEIZED**

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed), photocopies or other photographic form, and electrical, electronic, and magnetic form (such as CDs, DVDs, smart cards, thumb drives, camera memory cards, electronic notebooks, or any other storage medium) that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) which may be found on the SUBJECT DEVICES:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct, in any format or media;
2. Letters, emails, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;
3. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;
4. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;
5. Any and all address books, names, lists of names, telephone numbers, and addresses of minors;
6. Any and all diaries, notebooks, notes, non-pornographic pictures of children, and any other records reflecting personal contact or other activities with minors;
7. Digital devices and/or their components, which include, but are not limited to:
 - a. Any digital devices and storage device capable of being used to commit, further, or store evidence of the offense listed above;

1 b. Any digital devices used to facilitate the transmission, creation,
2 display, encoding or storage of data, including word processing equipment, modems,
3 docking stations, monitors, cameras, printers, encryption devices, and optical scanners;

4 c. Any magnetic, electronic, or optical storage device capable of
5 storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or
6 memory buffers, smart cards, PC cards, memory sticks, flashdrives, thumb drives, camera
7 memory cards, media cards, electronic notebooks, and personal digital assistants;

8 d. Any documentation, operating logs and reference manuals regarding
9 the operation of the digital device or software;

10 e. Any applications, utility programs, compilers, interpreters, and other
11 software used to facilitate direct or indirect communication with the computer hardware,
12 storage devices, or data to be searched;

13 f. Any physical keys, encryption devices, dongles and similar physical
14 items that are necessary to gain access to the computer equipment, storage devices or
15 data; and

16 g. Any passwords, password files, test keys, encryption codes or other
17 information necessary to access the computer equipment, storage devices or data;

18 8. Evidence of who used, owned or controlled any seized digital device(s) at
19 the time the things described in this warrant were created, edited, or deleted, such as logs,
20 registry entries, saved user names and passwords, documents, and browsing history;

21 9. Evidence of malware that would allow others to control any seized digital
22 device(s) such as viruses, Trojan horses, and other forms of malicious software, as well
23 as evidence of the presence or absence of security software designed to detect malware;
24 as well as evidence of the lack of such malware;

25 10. Evidence of the attachment to the digital device(s) of other storage devices
26 or similar containers for electronic evidence;

27 11. Evidence of counter-forensic programs (and associated data) that are
28 designed to eliminate data from a digital device;

12. Evidence of times the digital device(s) was used;

13. Any other electronically stored information (ESI) from the digital device(s) necessary to understand how the digital device was used, the purpose of its use, who used it, and when.

13. Communications concerning or intended to facilitate sexual contact with minors.

THE SEIZURE OF DIGITAL DEVICES AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES.